POLICY 3.00 PASSWORD PROTECTION

Information technology resources will be protected in accordance with Office for Information Resources (OIR) approved techniques.

PURPOSE:

To ensure information resources requiring password protection will employ reasonable identification and authentication techniques.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994

OBJECTIVES:

1. Minimize information technology risks through password protection methodologies and techniques.
2. Define user responsibilities for protecting information technology resources.
3. Promote the safeguarding of information technology resources in a cost effective manner such that the cost of security is commensurate with the value and sensitivity of the resources.

SCOPE:

The scope of this policy includes all information resource assets, such as applications, workstations, servers, printers, and personal digital assistants.

IMPLEMENTATION:

Office for Information Resources (OIR)

1. Develop, implement and maintain standards for acceptable information resource password protection.
2. Assign responsibility for ensuring compliance with password standards, procedures and guidelines.

Agency

1. Ensure password protection standards and guidelines are implemented and enforced.
2. Implement agency processes and procedures in support of State password policy and procedures.
3. Identify individual(s) responsible for ensuring compliance with password standards, procedures and guidelines.

4. Refrain from implementing agency procedures, processes or practices that would expose networked information resources to unnecessary or unauthorized risks.

Individual Users/Clients

1. Adhere to statewide and/or agency password and software policy, standards, procedures and guidelines.
2. Refrain from behaviors that would expose networked information technology resources to unnecessary or unauthorized risks.